

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

KOLSTER OY AB
Iso Roobertinkatu 23
P.O. Box 148
FIN-00121 Helsinki
FINLANDEDate of mailing (day/month/year)
29 November 2000 (29.11.00)Applicant's or agent's file reference
2980237PC/nu

IMPORTANT NOTIFICATION

International application No.
PCT/FI99/00462International filing date (day/month/year)
27 May 1999 (27.05.99)

1. The following indications appeared on record concerning:

☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative

Name and Address

ALMA MEDIA OYJ
Eteläesplanadi 14
FIN-00100 Helsinki
Finland

State of Nationality

FI

State of Residence

FI

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address

ALMA MEDIA OYJ
Eteläesplanadi 14
FIN-00130 Helsinki
Finland

State of Nationality

FI

State of Residence

FI

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office ☐ the designated Offices concerned
☐ the International Searching Authority ☒ the elected Offices concerned
☐ the International Preliminary Examining Authority ☐ other:The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

C. Cupello

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 29 February 2000 (29.02.00)	
International application No. PCT/FI99/00462	Applicant's or agent's file reference 2980237PC/nu
International filing date (day/month/year) 27 May 1999 (27.05.99)	Priority date (day/month/year) 29 May 1998 (29.05.98)
Applicant TURPEINEN, Marko et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

22 December 1999 (22.12.99)

☐ in a notice effecting later election filed with the International Bureau on:2. The election ☒ was☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

F. Baechler

Telephone No.: (41-22) 338.83.38

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS**

PCT

09 / 700928

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P1764P	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/DE 99/ 01365	Internationales Anmeldedatum (Tag/Monat/Jahr) 06/05/1999
(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 20/05/1998	
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.	

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbaren **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2.



Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3.



Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

**VERFAHREN UND ANORDNUNG ZUM RECHNERGESTÜTZTEN AUSTAUSCH KRYPTOGRAPHISCHER
SCHLÜSSEL ZWISCHEN EINER ERSTEN COMPUTEREINHEIT UND EINER ZWEITEN COMPUTER-
EINHEIT**

5. Hinsichtlich der Zusammenfassung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1A



wie vom Anmelder vorgeschlagen



keine der Abb.



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.

BEST AVAILABLE COPY

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 195 18 546 C (SIEMENS AG) 1. August 1996 (1996-08-01) in der Anmeldung erwähnt Spalte 1, Zeile 24 - Zeile 28 Spalte 4, Zeile 41 - Spalte 8, Zeile 45 ---	1, 2, 17, 20, 26-33, 48, 51, 57-62
X	DE 195 18 544 C (SIEMENS AG) 1. August 1996 (1996-08-01)	1, 17, 32, 48
A	Spalte 1, Zeile 24 - Zeile 28 Spalte 4, Zeile 46 - Spalte 10, Zeile 17 ---	12, 13, 43, 44
A	EP 0 661 844 A (IBM) 5. Juli 1995 (1995-07-05) Spalte 8, Zeile 51 - Spalte 11, Zeile 45; Abbildung 4 ---	1, 3, 4, 32, 34, 35
	--- -/--	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

5. November 1999

Absendedatum des internationalen Recherchenberichts

12/11/1999

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Holper, G

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>DIFFIE W ET AL: "AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES" DESIGNS, CODES AND CRYPTOGRAPHY, Bd. 2, Nr. 2, 1. Juni 1992 (1992-06-01), Seiten 107-125, XP000653208 ISSN: 0925-1022 in der Anmeldung erwähnt Seite 114, Absatz 2 -Seite 116, Absatz 1 -----</p>	1,32

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 99/01365

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19518546 C	01-08-1996	CN 1186579 A WO 9637064 A EP 0872076 A JP 11505384 T	01-07-1998 21-11-1996 21-10-1998 18-05-1999
DE 19518544 C	01-08-1996	CN 1186579 A WO 9637064 A EP 0872076 A JP 11505384 T	01-07-1998 21-11-1996 21-10-1998 18-05-1999
EP 0661844 A	05-07-1995	US 5491749 A DE 69416809 D DE 69416809 T JP 2926699 B JP 7212356 A	13-02-1996 08-04-1999 07-10-1999 28-07-1999 11-08-1995

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

09/700928

PCT

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

An
SIEMENS AG
Postfach 22 16 34
D-80333 München
GERMANY

YT GG VM Mch P/Ri
Eing. 17. Nov. 1999
GR
Frist

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES
INTERNATIONALEN RECHERCHENBERICHTS
ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

Absenddatum
(Tag/Monat/Jahr)

12/11/1999

Aktenzeichen des Anmelders oder Anwalts

GR 98P1764P

WEITERES VORGEHEN

siehe Punkte 1 und 4 unten

Internationales Aktenzeichen

PCT/DE 99/01365

Internationales Anmeldedatum

(Tag/Monat/Jahr)

06/05/1999

Anmelder

SIEMENS AKTIENGESELLSCHAFT et al.

1. ☒ Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

Einreichung von Änderungen und einer Erklärung nach Artikel 19:

Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

Bis wann sind Änderungen einzureichen?

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

Wo sind Änderungen einzureichen?

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20.
Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. ☐ Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.

3. ☐ Hinsichtlich des Widerspruchs gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß

☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.

☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von 18 Monaten seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90 bis bzw. 90.3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von 19 Monaten seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von 20 Monaten seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Annick Crab

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.

Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen die anderen Ansprüche nicht neu nummeriert zu werden. Im Fall einer Neunummerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
"Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt. "Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigefügt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS**

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P1764P	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/DE 99/ 01365	Internationales Anmeldedatum (Tag/Monat/Jahr) 06/05/1999	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 20/05/1998
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. ☐ **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

**VERFAHREN UND ANORDNUNG ZUM RECHNERGESTÜTZTEN AUSTAUSCH KRYPTOGRAPHISCHER
SCHLÜSSEL ZWISCHEN EINER ERSTEN COMPUTEREINHEIT UND EINER ZWEITEN COMPUTER-
EINHEIT**

5. Hinsichtlich der Zusammenfassung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1A



wie vom Anmelder vorgeschlagen



keine der Abb.



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 195 18 546 C (SIEMENS AG) 1. August 1996 (1996-08-01) in der Anmeldung erwähnt Spalte 1, Zeile 24 - Zeile 28 Spalte 4, Zeile 41 - Spalte 8, Zeile 45 ---	1, 2, 17, 20, 26-33, 48, 51, 57-62
X	DE 195 18 544 C (SIEMENS AG) 1. August 1996 (1996-08-01)	1, 17, 32, 48
A	Spalte 1, Zeile 24 - Zeile 28 Spalte 4, Zeile 46 - Spalte 10, Zeile 17 ---	12, 13, 43, 44
A	EP 0 661 844 A (IBM) 5. Juli 1995 (1995-07-05) Spalte 8, Zeile 51 - Spalte 11, Zeile 45; Abbildung 4 ---	1, 3, 4, 32, 34, 35
	--- -/-	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie*** Besondere Kategorien von angegebenen Veröffentlichungen :**

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

5. November 1999

Absendedatum des internationalen Recherchenberichts

12/11/1999

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Holper, G

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>DIFFIE W ET AL: "AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES" DESIGNS, CODES AND CRYPTOGRAPHY, Bd. 2, Nr. 2, 1. Juni 1992 (1992-06-01), Seiten 107-125, XP000653208 ISSN: 0925-1022 in der Anmeldung erwähnt Seite 114, Absatz 2 -Seite 116, Absatz 1 -----</p>	1,32

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 99/01365

Im Recherchenbericht angeführtes Patendokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19518546 C	01-08-1996	CN 1186579 A	01-07-1998
		WO 9637064 A	21-11-1996
		EP 0872076 A	21-10-1998
		JP 11505384 T	18-05-1999
DE 19518544 C	01-08-1996	CN 1186579 A	01-07-1998
		WO 9637064 A	21-11-1996
		EP 0872076 A	21-10-1998
		JP 11505384 T	18-05-1999
EP 0661844 A	05-07-1995	US 5491749 A	13-02-1996
		DE 69416809 D	08-04-1999
		DE 69416809 T	07-10-1999
		JP 2926699 B	28-07-1999
		JP 7212356 A	11-08-1995

01-07-1998
 21-11-1996
 21-10-1998
 18-05-1999
 01-07-1998
 21-11-1996
 21-10-1998
 18-05-1999
 13-02-1996
 08-04-1999
 07-10-1999
 28-07-1999
 11-08-1995

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

09/700928

PCT

REC'D 17 JUL 2000

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P1764P	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE99/01365	Internationales Anmeldedatum (Tag/Monat/Jahr) 06/05/1999	Prioritätsdatum (Tag/Monat/Jahr) 20/05/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		



- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

☒ Außerdem liegen dem Bericht **ANLAGEN** bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

 Diese Anlagen umfassen insgesamt 8 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 26/11/1999	Datum der Fertigstellung dieses Berichts 13.07.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Pajatakis, E Tel. Nr. +49 89 2399 8898 

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE99/01365

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-38 ursprüngliche Fassung

Patentansprüche, Nr.:

1 (Teil), 2-31, 32 (Teil), ursprüngliche Fassung
34 (Teil), 35-62

1 (Teil), 32 (Teil), eingereicht bei der persönlichen Rücksprache am 07/07/2000
33, 34 (Teil)

Zeichnungen, Blätter:

1/6-6/6 eingegangen am 23/08/1999 mit Schreiben vom 09/08/1999

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-62
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-62
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-62
	Nein: Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Der Gegenstand des Anspruchs 1 ist neu und erfinderisch (Artikel 33(2)(3)).

1.1 Der Anspruch 1 betrifft ein Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit .

Ein derartiges Verfahren ist aus **D1 = DE 195 18 546 C** (in der Anmeldung erwähnt) bei dem aus einer ersten Zufallszahl mit Hilfe eines erzeugenden Elements einer endlichen Gruppe in der ersten Computereinheit ein erster Wert g^t gebildet wird. Eine Nachricht M1 wird von der ersten Computereinheit an die zweite Computereinheit übertragen wird, wobei die Nachricht M1 den einen Wert g^t aufweist. In der zweiten Computereinheit wird ein Sitzungsschlüssel K mit Hilfe einer Hash-Funktion h1 gebildet wobei eine erste Eingangsgröße der Hash-Funktion h1 einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts g^t mit einem geheimen Netzschlüssel s. In der ersten Computereinheit wird der Sitzungsschlüssel K gebildet mit Hilfe der Hash-Funktion h1, wobei eine zweite Eingangsgröße der Hash-Funktion h1 einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels g^s mit der Zufallszahl t. In der ersten Computereinheit wird mit Hilfe einer weiteren Hash-Funktion h2 eine vierte Eingangsgröße gebildet, wobei eine dritte Eingangsgröße für die Hash-Funktion h2 zur Bildung der vierten Eingangsgröße weitere Größen aufweist. In der ersten Computereinheit wird ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet unter Anwendung einer Signaturfunktion SigU. Eine weitere Nachricht M3 von wird der ersten Computereinheit an die zweite Computereinheit übertragen, wobei die weitere Nachricht M3 den Signaturterm SigU aufweist, und bei der zweiten Computereinheit wird der Signaturterm verifiziert.

1.2 Der Gegenstand des Anspruchs 1 unterscheidet sich von **D1** in dem die Hash-Funktion h2 nicht den Sitzungsschlüssel als Eingangsgröße hat, sondern Größen aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden

kann. Ein Bestandteil der Größen, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, ist nicht öffentlich.

Dadurch wird eine Erhöhung der Sicherheit beim Austausch von Schlüsseln erreicht. Die Auswahl dieser Maßnahme hat den zusätzlichen Effekt zur Folge, daß für eine Verifikation der Signatur der Sitzungsschlüssel nicht gespeichert werden braucht. Dadurch ergibt sich ein veringertes sicherungstechnischer Aufwand bei dem Aufbau des Speichers.

- 1.3 Ein derartiges Vorgehen wird durch den Stand der Technik nicht nahegelegt.

Sowohl **D1** als auch **DE19518544** leiten weg, weil es vorgeschlagen wird den Sitzungsschlüssel K selbst zu signieren und zu übertragen.

Ebenso wird in **DIFFIE W ET AL: 'AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES' DESIGNS, CODES AND CRYPTOGRAPHY, Bd. 2, Nr. 2, 1. Juni 1992 (1992-06-01), Seiten 107-125, ISSN: 0925-1022** vorgeschlagen den Sitzungsschlüssel K auszutauschen.

2. Die obengenannte Feststellung gilt auch für den Anspruch 32, der dem Anspruch 1 entspricht.
3. Die abhängigen Ansprüche betreffen spezielle Ausführungen des Gegenstands der obengenannten unabhängigen Ansprüche und sind demnach ebenso neu und erfinderisch.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

1. Die unabhängigen Ansprüche sind nicht in der zweiteiligen Form gegenüber **D1** sein (Regel 6.3(b)).

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

1. In den Ansprüchen 1 und 32 sind die Nachrichten nicht stetig numeriert. Es wird von der ersten zur dritten Nachricht übergegangen. Dadurch entstehen Zweifel über den Schutzbereich.

Die Anmelderin ist der Auffassung, daß "*erste Nachricht*", "*zweite Nachricht*" usw. lediglich eine frei gewählte Bezeichnung der Nachrichten darstellen. Dieser Auffassung kann nicht zugestimmt werden, weil es sich eindeutig um eine fortlaufende Numerierung handelt (vgl. auch Richtlinien III, 4.2).

2. Aus den Ansprüchen 4 und 35 ist nicht klar herausgestellt welche von den in den vorausgehenden Ansprüchen definierten Größen gemeint sind.

Gemäß der Anmelderin handelt es sich um die Größen aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann. Dies ist jedoch nicht in den Ansprüchen 4 und 35 erwähnt.

Patentansprüche

1. Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit (U) und einer zweiten Computereinheit (N),
 - bei dem aus einer ersten Zufallszahl (t) mit Hilfe eines erzeugenden Elements (g) einer endlichen Gruppe in der ersten Computereinheit (U) ein erster Wert (g^t) gebildet wird,
 - bei dem eine erste Nachricht (M1) von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen wird, wobei die erste Nachricht (M1) mindestens den ersten Wert (g^t) aufweist,
 - bei dem in der zweiten Computereinheit (N) ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h1) gebildet wird, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit einem geheimen Netzschlüssel (s),
 - bei dem in der ersten Computereinheit (U) der Sitzungsschlüssel (K) gebildet wird mit Hilfe der ersten Hash-Funktion (h1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels (g^S) mit der ersten Zufallszahl (t),
 - bei dem in der ersten Computereinheit (U) mit Hilfe einer zweiten Hash-Funktion (h2) oder der ersten Hash-Funktion (h1) eine vierte Eingangsgröße gebildet wird, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße eine oder weitere Größen aufweist, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, *wobei zumindest ein Teil der Größe eine nicht öffentliche Größe ist,*
 - bei dem in der ersten Computereinheit (U) ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet wird unter Anwendung einer ersten Signaturfunktion (Sig_U),

- bei der ersten Nachricht (M1) mindestens den ersten Wert (g^t) aufweist,
- in der zweiten Computereinheit (N) wird ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h1) gebildet, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit einem geheimen Netzschlüssel (s),
 - in der ersten Computereinheit (U) wird der Sitzungsschlüssel (K) gebildet mit Hilfe der ersten Hash-Funktion (h1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels (g^S) mit der ersten Zufallszahl (t),
 - in der ersten Computereinheit (U) wird mit Hilfe einer zweiten Hash-Funktion (h2) oder der ersten Hash-Funktion (h1) eine vierte Eingangsgröße gebildet, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße eine oder weitere Größen aufweist, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, wobei zumindest ein Teil der Größe eine nicht öffentliche Größe ist,
 - in der ersten Computereinheit (U) wird ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet unter Anwendung einer ersten Signaturfunktion (Sig),
 - eine dritte Nachricht (M3) wird von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen, wobei die dritte Nachricht (M3) mindestens den Signaturterm der ersten Computereinheit (U) aufweist, und
 - in der zweiten Computereinheit (N) wird der Signaturterm verifiziert.

33. Anordnung nach Anspruch 31,
bei dem der geheime Netzschlüssel und/oder der öffentliche Netzschlüssel langlebige Schlüssel ist/sind.

34. Anordnung nach Anspruch 32 oder 33,

FIG 1A

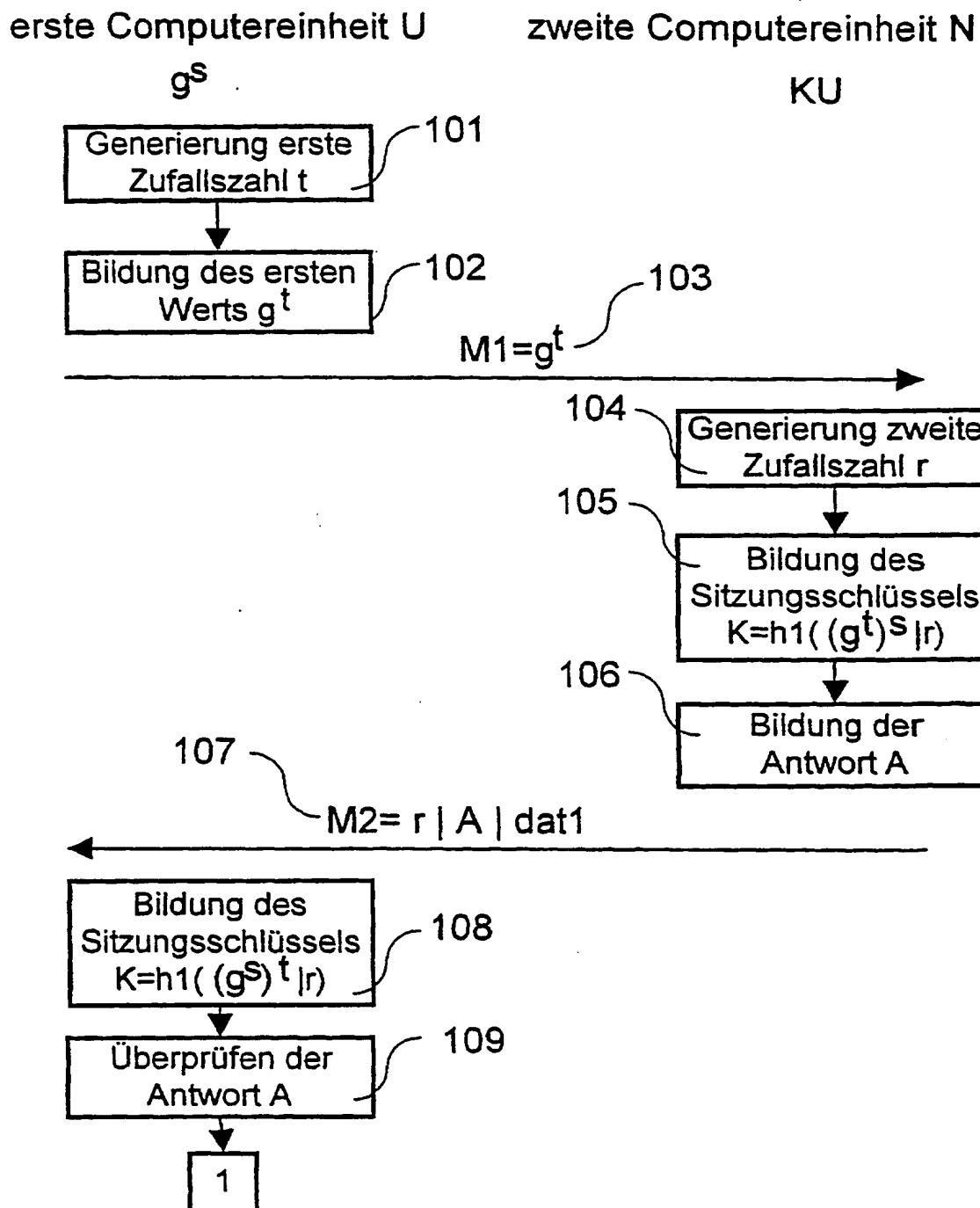
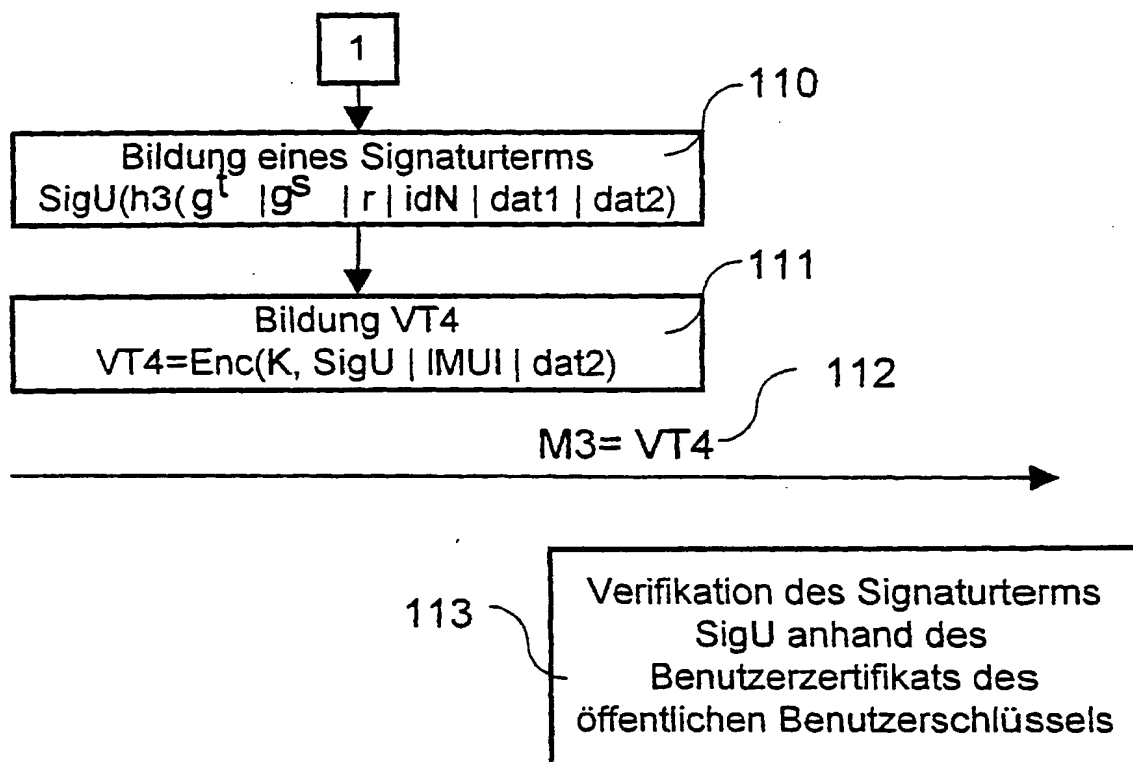


FIG 1B

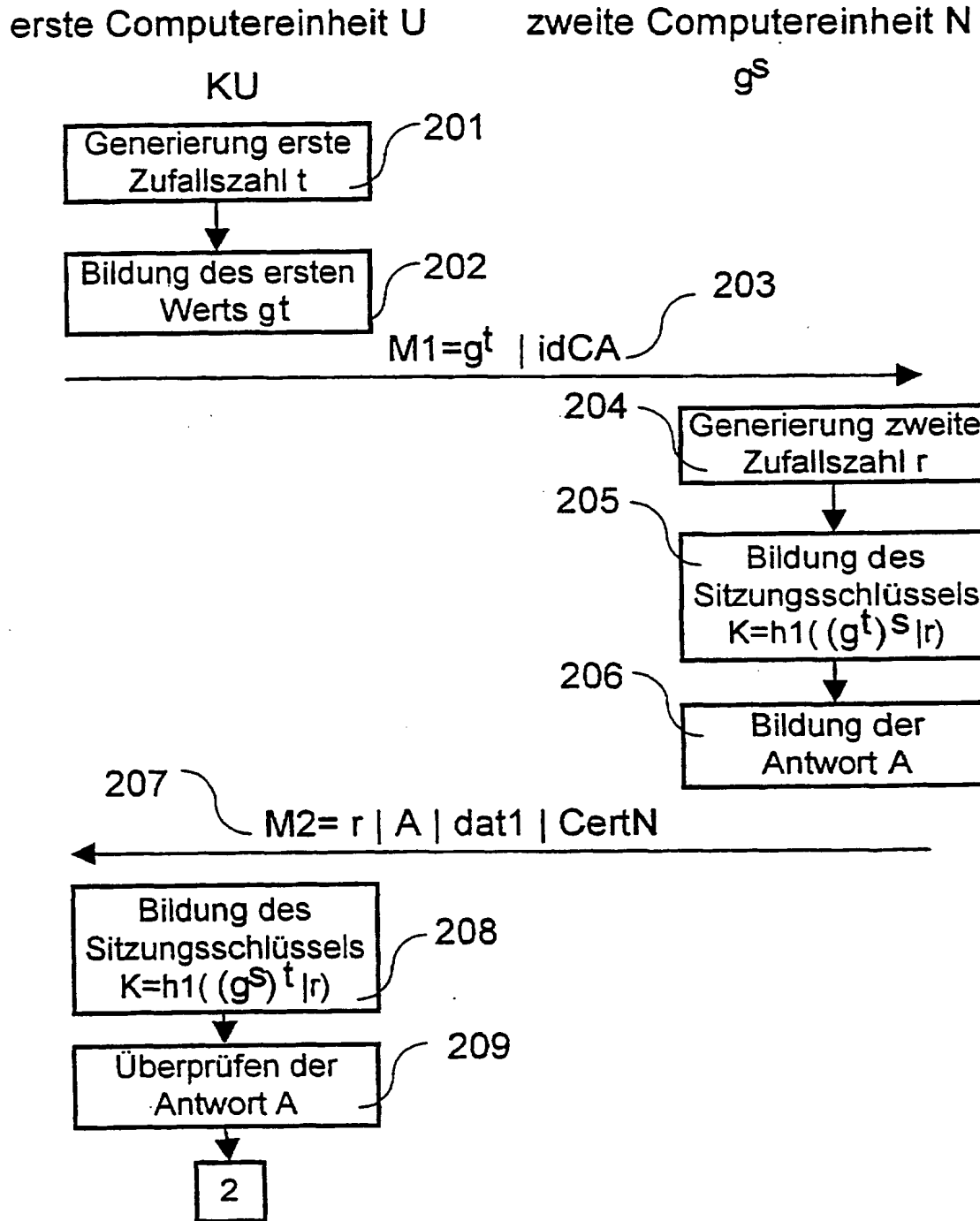
erste Computereinheit U

zweite Computereinheit N



3 / 6

FIG 2A

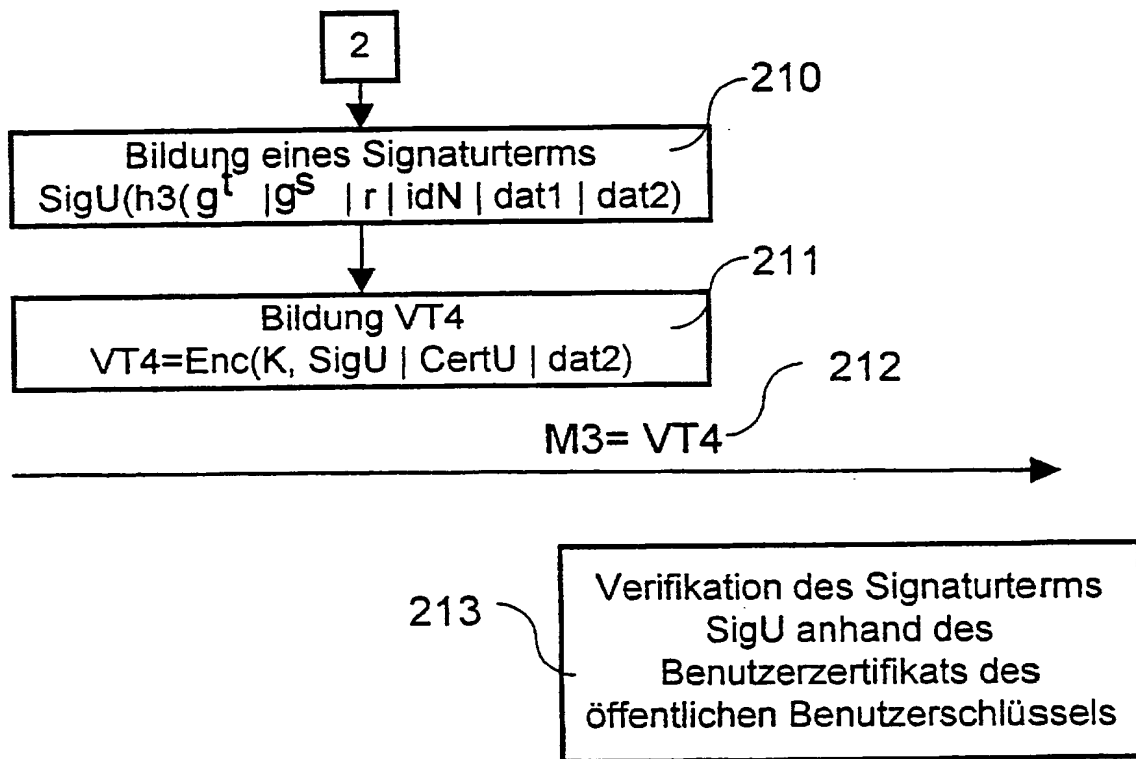


4/6

FIG 2B

erste Computereinheit U

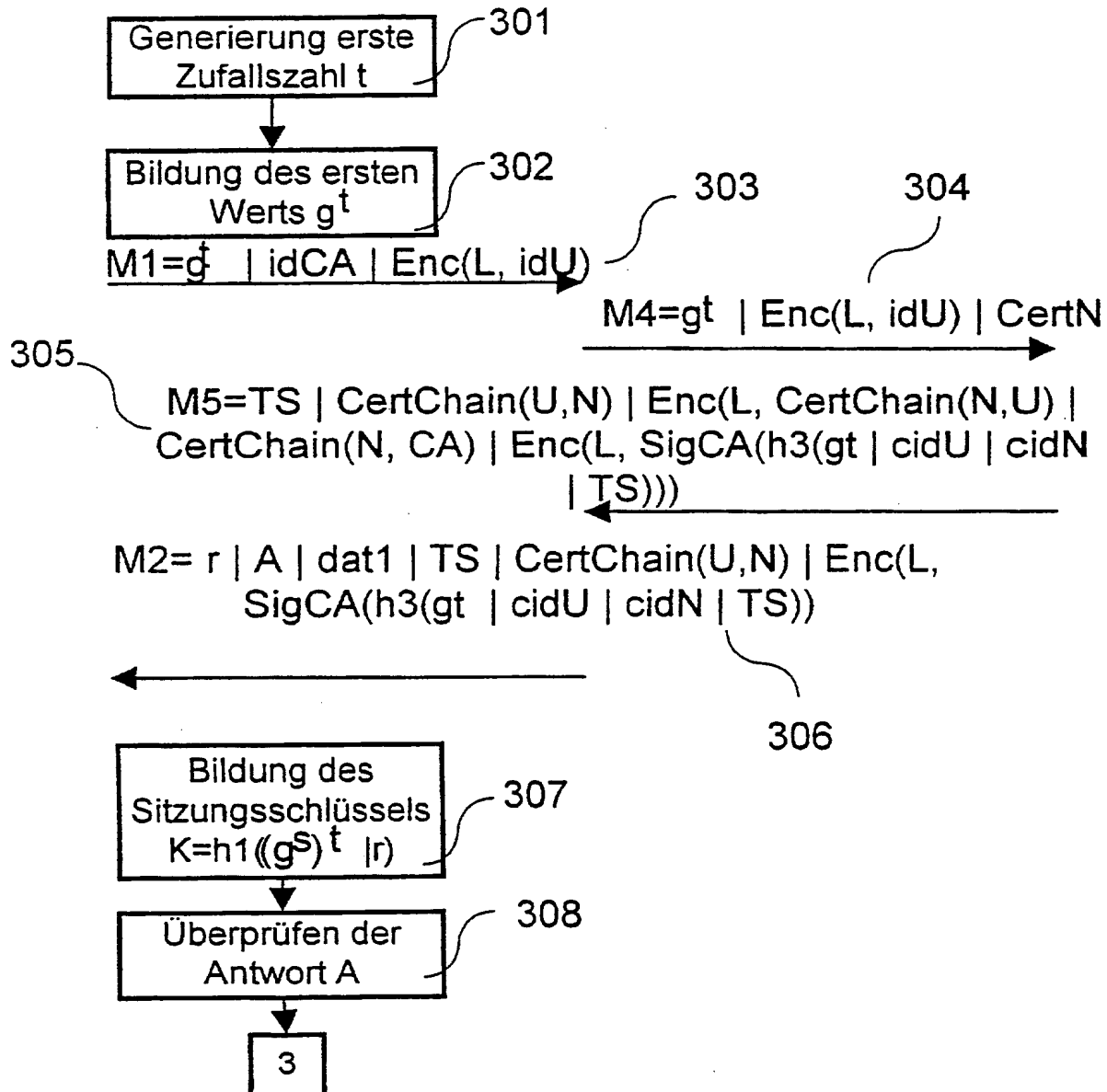
zweite Computereinheit N



5 / 6

FIG 3A

erste Computereinheit U Zertifizierungscomputereinheit CA
 g^U zweite Computereinheit N

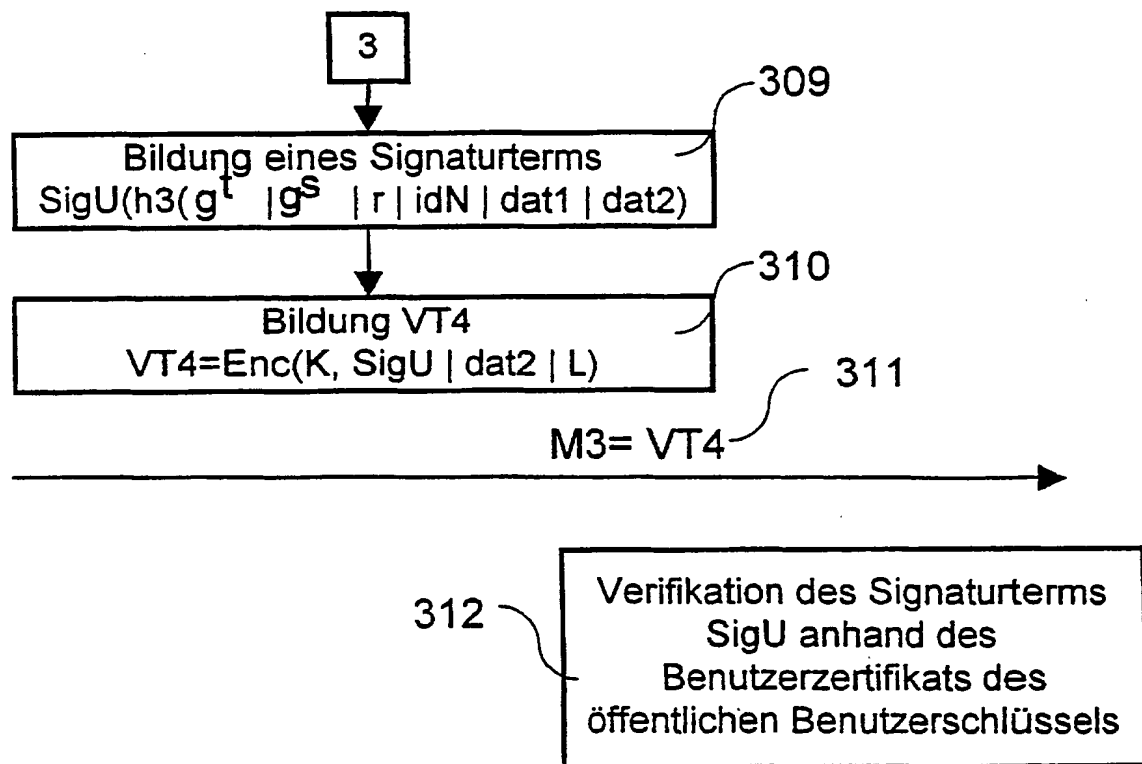


6 / 6

FIG 3B

erste Computereinheit U

zweite Computereinheit N



3
4
Translation
09/700928

PATENT COOPERATION TREATY

09/700928 #3

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GR 98P1764P	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE99/01365	International filing date (day/month/year) 06 May 1999 (06.05.99)	Priority date (day/month/year) 20 May 1998 (20.05.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 26 November 1999 (26.11.99)	Date of completion of this report 13 July 2000 (13.07.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE99/01365

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

- ☐ the international application as originally filed.
- ☒ the description, pages 1-38, as originally filed,
 pages _____, filed with the demand,
 pages _____, filed with the letter of _____,
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. 1(partly),2-31,32(partly),34(partly),35-62, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. 1(partly),32(partly),33,34(partly), filed with the letter of 07 July 2000 (07.07.2000),
 Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig _____, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig 1/6-6/6, filed with the letter of 09 August 1999 (09.08.1999),
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

 International application No.
 PCT/DE 99/01365

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-62	YES
	Claims		NO
Inventive step (IS)	Claims	1-62	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-62	YES
	Claims		NO

2. Citations and explanations

1. The subject matter of Claim 1 is novel and inventive (Article 33(2) and (3)).

1.1 Claim 1 relates to a method for the computer-assisted exchange of cryptographic keys between a first computer unit and a second computer unit.

DE 195 18 546 C (D1) (cited in the application) discloses a method of this kind according to which a first value g^t is generated in the first computer unit from a first random number with the aid of a generating element of a finite group. A message M_1 having the above first value g^t is transmitted from the first computer unit to the second computer unit. In the second computer unit a session key K is generated with the aid of a hash function h_1 , with a first input variable of the hash function h_1 having a first term which is formed by exponentiation of the first value g^t with a secret network key s . In the first computer unit the session key K is generated with the aid of the hash function h_1 , with a second input variable of said hash function h_1 having a second term which is formed by exponentiation of a public network key g^s with the

random number t . In the first computer unit a fourth input variable is generated with the aid of another hash function $h2$, with a third input variable for the hash function $h2$ having additional variables for the generation of the fourth input variable. In the first computer unit a signature term is generated from at least the fourth input variable by means of a signature function $SigU$. Another message $M3$ is transmitted from the first computer unit to the second computer unit, said further message $M3$ having the signature term $SigU$ which is then verified by the second computer unit.

- 1.2 The subject matter of Claim 1 differs from **D1** in that the input variable for the hash function $h2$ is not the session key but variables from which the session key can be unequivocally inferred. No component of those variables from which the session key can be unequivocally inferred is public.

This improves security in the exchange of keys. An added effect of this measure is that the session key does not have to be memorized for verification of the signature. This reduces the outlay for memory to secure the system.

- 1.3 The prior art does not suggest a process of the type described above.

Both **D1** and **DE 195 18 544** suggest a different direction because they provide for the session key K itself to be signed and transmitted.

Similarly, **DIFFIE W ET AL: 'AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES', DESIGNS, CODES AND**

CRYPTOGRAPHY, vol. 2, no.2, 1 June 1992 (1992-06-01), pp. 107-125, ISSN: 0925-1022, suggests that the session key K should be exchanged.

2. The above statement also applies to Claim 32, which corresponds to Claim 1.
3. The dependent claims relate to special embodiments of the subject matter of the above independent claims and are therefore also novel and inventive.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 99/01365

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. The independent claims were not written in two-part form with respect to **D1** (Rule 6.3)(b)).

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. The messages referred to in Claims 1 and 32 are not numbered consecutively, the text moving directly from the first message to the third. This creates uncertainty as to the scope of protection.

The Applicant considers that "first message", "second message", etc. are merely randomly chosen designations of the messages. This argument cannot be accepted since the numbering is clearly consecutive (see also Guidelines III, 4.2)

2. Claims 4 and 35 do not indicate clearly to which of the variables defined in the preceding claims they refer.

According to the Applicant, Claims 4 and 35 refer to those variables from which the session key can be unequivocally inferred. This, however, is not mentioned in said claims.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

09/700928

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN
PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SIEMENS AKTIENGESELLSCHAFT
Postfach 22 16 34
D-80506 München
ALLEMAGNE

PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG
DES INTERNATIONALEN VORLÄUFIGEN
PRÜFUNGSBERICHTS
(Regel 71.1 PCT)

Absendedatum
(Tag/Monat/Jahr) 13.07.2000

Aktenzeichen des Anmelders oder Anwalts
GR 98P1764P

WICHTIGE MITTEILUNG

Internationales Aktenzeichen
PCT/DE99/01365

Internationales Anmeldedatum (Tag/Monat/Jahr)
06/05/1999

Prioritätsdatum (Tag/Monat/Jahr)
20/05/1998

Anmelder
SIEMENS AKTIENGESELLSCHAFT et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde



Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Scaglia, F

Tel. +49 89 2399-2836



VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P1764P	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE99/01365	Internationales Anmeldedatum (Tag/Monat/Jahr) 06/05/1999	Prioritätsdatum (Tag/Monat/Tag) 20/05/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		



1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 8 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

I ☒ Grundlage des Berichts
II ☐ Priorität
III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
IV ☐ Mangelnde Einheitlichkeit der Erfindung
V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
VI ☐ Bestimmte angeführte Unterlagen
VII ☒ Bestimmte Mängel der internationalen Anmeldung
VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 26/11/1999	Datum der Fertigstellung dieses Berichts 13.07.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Pajatakis, E Tel. Nr. +49 89 2399 8898 

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE99/01365

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-38 ursprüngliche Fassung

Patentansprüche, Nr.:

1 (Teil), 2-31, 32 (Teil), ursprüngliche Fassung
34 (Teil), 35-62

1 (Teil), 32 (Teil), eingereicht bei der persönlichen Rücksprache am 07/07/2000
33, 34 (Teil)

Zeichnungen, Blätter:

1/6-6/6 eingegangen am 23/08/1999 mit Schreiben vom 09/08/1999

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-62
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-62
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-62
	Nein: Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Der Gegenstand des Anspruchs 1 ist neu und erfinderisch (Artikel 33(2)(3)).

1.1 Der Anspruch 1 betrifft ein Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit .

Ein derartiges Verfahren ist aus **D1 = DE 195 18 546 C** (in der Anmeldung erwähnt) bei dem aus einer ersten Zufallszahl mit Hilfe eines erzeugenden Elements einer endlichen Gruppe in der ersten Computereinheit ein erster Wert g^t gebildet wird. Eine Nachricht M1 wird von der ersten Computereinheit an die zweite Computereinheit übertragen wird, wobei die Nachricht M1 den einen Wert g^t aufweist. In der zweiten Computereinheit wird ein Sitzungsschlüssel K mit Hilfe einer Hash-Funktion h1 gebildet wobei eine erste Eingangsgröße der Hash-Funktion h1 einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts g^t mit einem geheimen Netzschlüssel s. In der ersten Computereinheit wird der Sitzungsschlüssel K gebildet mit Hilfe der Hash-Funktion h1, wobei eine zweite Eingangsgröße der Hash-Funktion h1 einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels g^s mit der Zufallszahl t. In der ersten Computereinheit wird mit Hilfe einer weiteren Hash-Funktion h2 eine vierte Eingangsgröße gebildet, wobei eine dritte Eingangsgröße für die Hash-Funktion h2 zur Bildung der vierten Eingangsgröße weitere Größen aufweist. In der ersten Computereinheit wird ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet unter Anwendung einer Signaturfunktion SigU. Eine weitere Nachricht M3 von wird der ersten Computereinheit an die zweite Computereinheit übertragen, wobei die weitere Nachricht M3 den Signaturterm SigU aufweist, und bei der zweiten Computereinheit wird der Signaturterm verifiziert.

1.2 Der Gegenstand des Anspruchs 1 unterscheidet sich von **D1** in dem die Hash-Funktion h2 nicht den Sitzungsschlüssel als Eingangsgröße hat, sondern Größen aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden

kann. Ein Bestandteil der Größen, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, ist nicht öffentlich.

Dadurch wird eine Erhöhung der Sicherheit beim Austausch von Schlüsseln erreicht. Die Auswahl dieser Maßnahme hat den zusätzlichen Effekt zur Folge, daß für eine Verifikation der Signatur der Sitzungsschlüssel nicht gespeichert werden braucht. Dadurch ergibt sich ein veringertes sicherungstechnischer Aufwand bei dem Aufbau des Speichers.

- 1.3 Ein derartiges Vorgehen wird durch den Stand der Technik nicht nahegelegt.

Sowohl **D1** als auch **DE19518544** leiten weg, weil es vorgeschlagen wird den Sitzungsschlüssel K selbst zu signieren und zu übertragen.

Ebenso wird in **DIFFIE W ET AL: 'AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES' DESIGNS, CODES AND CRYPTOGRAPHY, Bd. 2, Nr. 2, 1. Juni 1992 (1992-06-01), Seiten 107-125, ISSN: 0925-1022** vorgeschlagen den Sitzungsschlüssel K auszutauschen.

2. Die obengenannte Feststellung gilt auch für den Anspruch 32, der dem Anspruch 1 entspricht.
3. Die abhängigen Ansprüche betreffen spezielle Ausführungen des Gegenstands der obengenannten unabhängigen Ansprüche und sind demnach ebenso neu und erfinderisch.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

1. Die unabhängigen Ansprüche sind nicht in der zweiteiligen Form gegenüber **D1** sein (Regel 6.3(b)).

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

1. In den Ansprüchen 1 und 32 sind die Nachrichten nicht stetig numeriert. Es wird von der ersten zur dritten Nachricht übergegangen. Dadurch entstehen Zweifel über den Schutzbereich.

Die Anmelderin ist der Auffassung, daß "*erste Nachricht*", "*zweite Nachricht*" usw. lediglich eine frei gewählte Bezeichnung der Nachrichten darstellen. Dieser Auffassung kann nicht zugestimmt werden, weil es sich eindeutig um eine fortlaufende Numerierung handelt (vgl. auch Richtlinien III, 4.2).

2. Aus den Ansprüchen 4 und 35 ist nicht klar herausgestellt welche von den in den vorausgehenden Ansprüchen definierten Größen gemeint sind.

Gemäß der Anmelderin handelt es sich um die Größen aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann. Dies ist jedoch nicht in den Ansprüchen 4 und 35 erwähnt.

Patentansprüche

1. Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer ersten Computereinheit (U) und einer zweiten Computereinheit (N),
- bei dem aus einer ersten Zufallszahl (t) mit Hilfe eines erzeugenden Elements (g) einer endlichen Gruppe in der ersten Computereinheit (U) ein erster Wert (g^t) gebildet wird,
 - bei dem eine erste Nachricht (M1) von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen wird, wobei die erste Nachricht (M1) mindestens den ersten Wert (g^t) aufweist,
 - bei dem in der zweiten Computereinheit (N) ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h1) gebildet wird, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit einem geheimen Netzschlüssel (s),
 - bei dem in der ersten Computereinheit (U) der Sitzungsschlüssel (K) gebildet wird mit Hilfe der ersten Hash-Funktion (h1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels (g^S) mit der ersten Zufallszahl (t),
 - bei dem in der ersten Computereinheit (U) mit Hilfe einer zweiten Hash-Funktion (h2) oder der ersten Hash-Funktion (h1) eine vierte Eingangsgröße gebildet wird, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße eine oder weitere Größen aufweist, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, wobei zumindest ein Teil der Größe eine nicht öffentliche Größe ist,
 - bei dem in der ersten Computereinheit (U) ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet wird unter Anwendung einer ersten Signaturfunktion (SigU),

- bei die ersten Nachricht (M_1) mindestens den ersten Wert (g^t) aufweist,
- in der zweiten Computereinheit (N) wird ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h_1) gebildet, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h_1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit einem geheimen Netzschlüssel (s),
 - in der ersten Computereinheit (U) wird der Sitzungsschlüssel (K) gebildet mit Hilfe der ersten Hash-Funktion (h_1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h_1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels (g^S) mit der ersten Zufallszahl (t),
 - in der ersten Computereinheit (U) wird mit Hilfe einer zweiten Hash-Funktion (h_2) oder der ersten Hash-Funktion (h_1) eine vierte Eingangsgröße gebildet wird, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h_1) oder für die zweite Hash-Funktion (h_2) zur Bildung der vierten Eingangsgröße eine oder weitere Größen aufweist, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, *wobei zumindest ein Teil der Größe eine nicht öffentliche Größe ist,*
 - in der ersten Computereinheit (U) wird ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet unter Anwendung einer ersten Signaturfunktion (Sig),
 - eine dritte Nachricht (M_3) wird von der ersten Computereinheit (U) an die zweite Computereinheit (N) übertragen, wobei die dritte Nachricht (M_3) mindestens den Signaturterm der ersten Computereinheit (U) aufweist, und
 - in der zweiten Computereinheit (N) wird der Signaturterm verifiziert.

33. Anordnung nach Anspruch 31,
bei dem der geheime Netzschlüssel und/oder der öffentliche Netzschlüssel langlebige Schlüssel ist/sind.

34. Anordnung nach Anspruch 32 oder 33,

FIG 1A

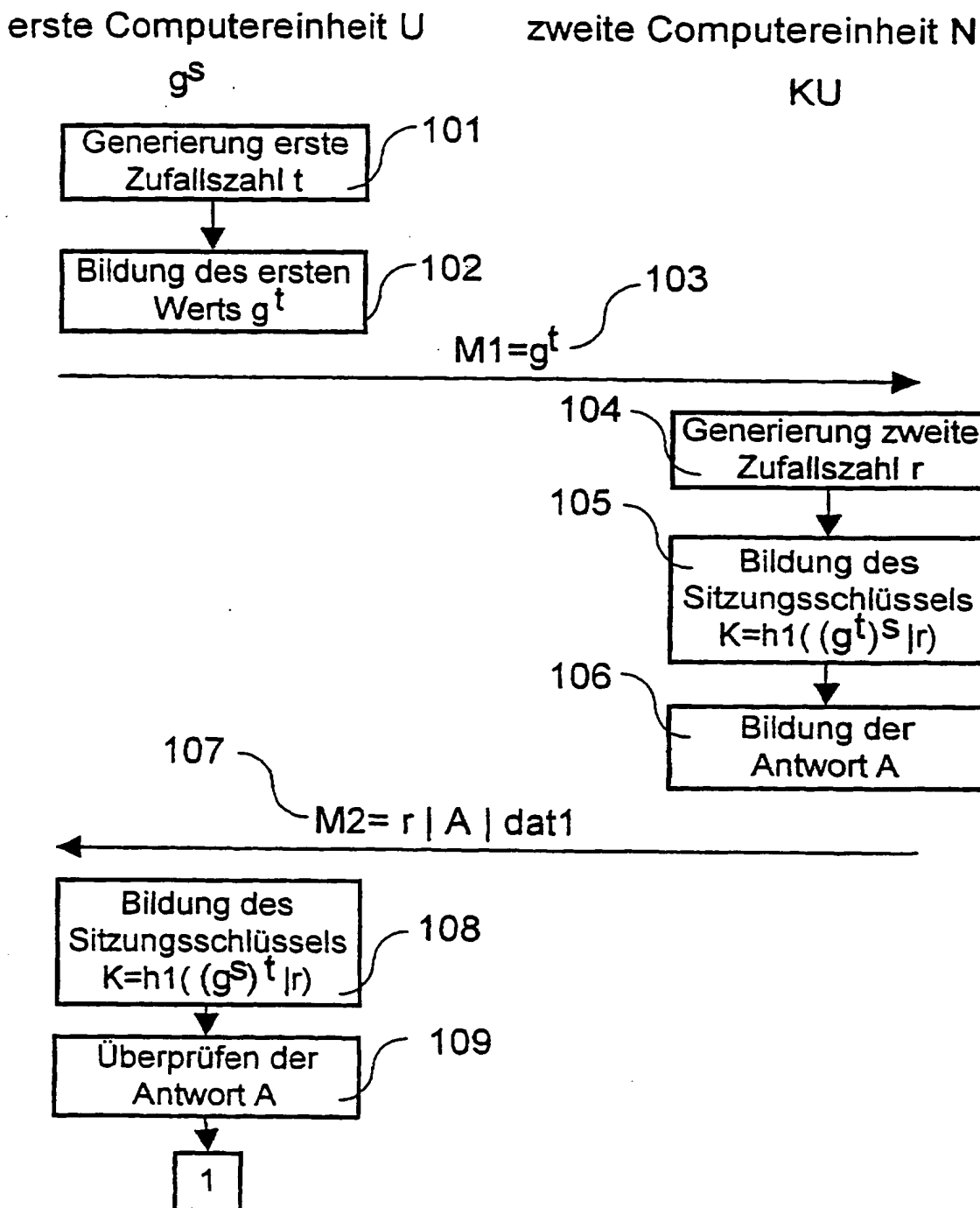


FIG 1B

erste Computereinheit U

zweite Computereinheit N

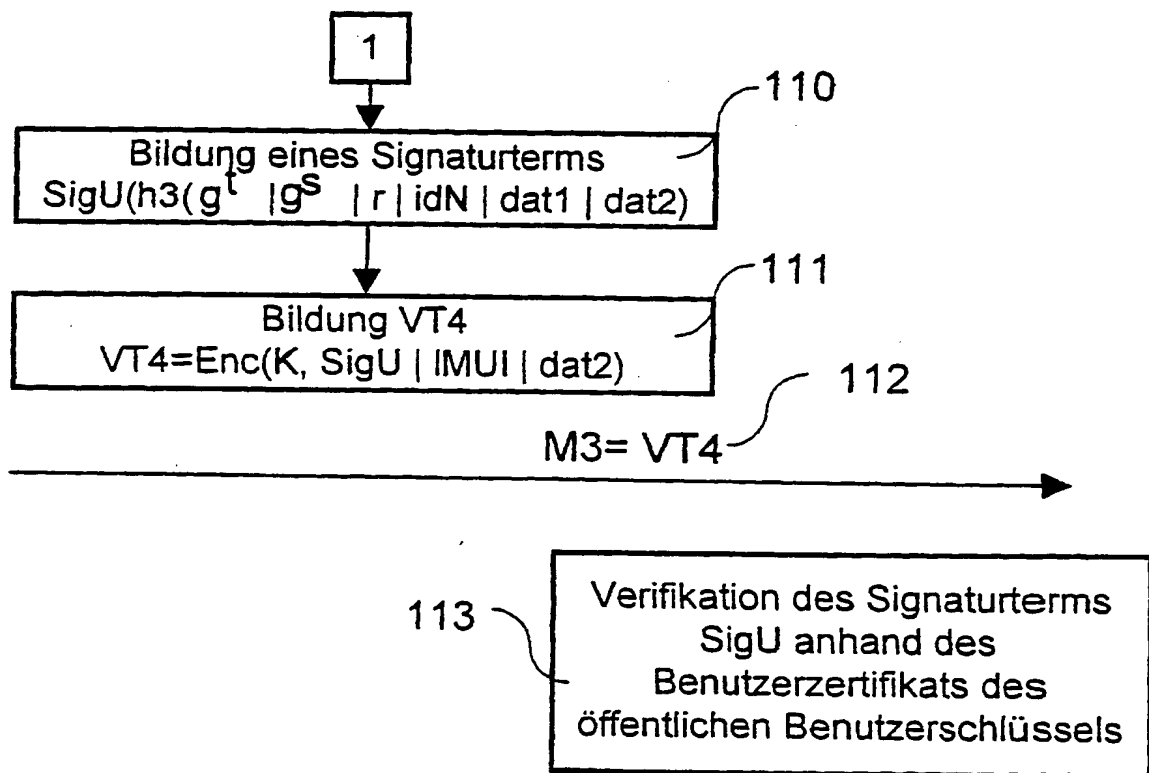


FIG 2A

erste Computereinheit U

zweite Computereinheit N

KU

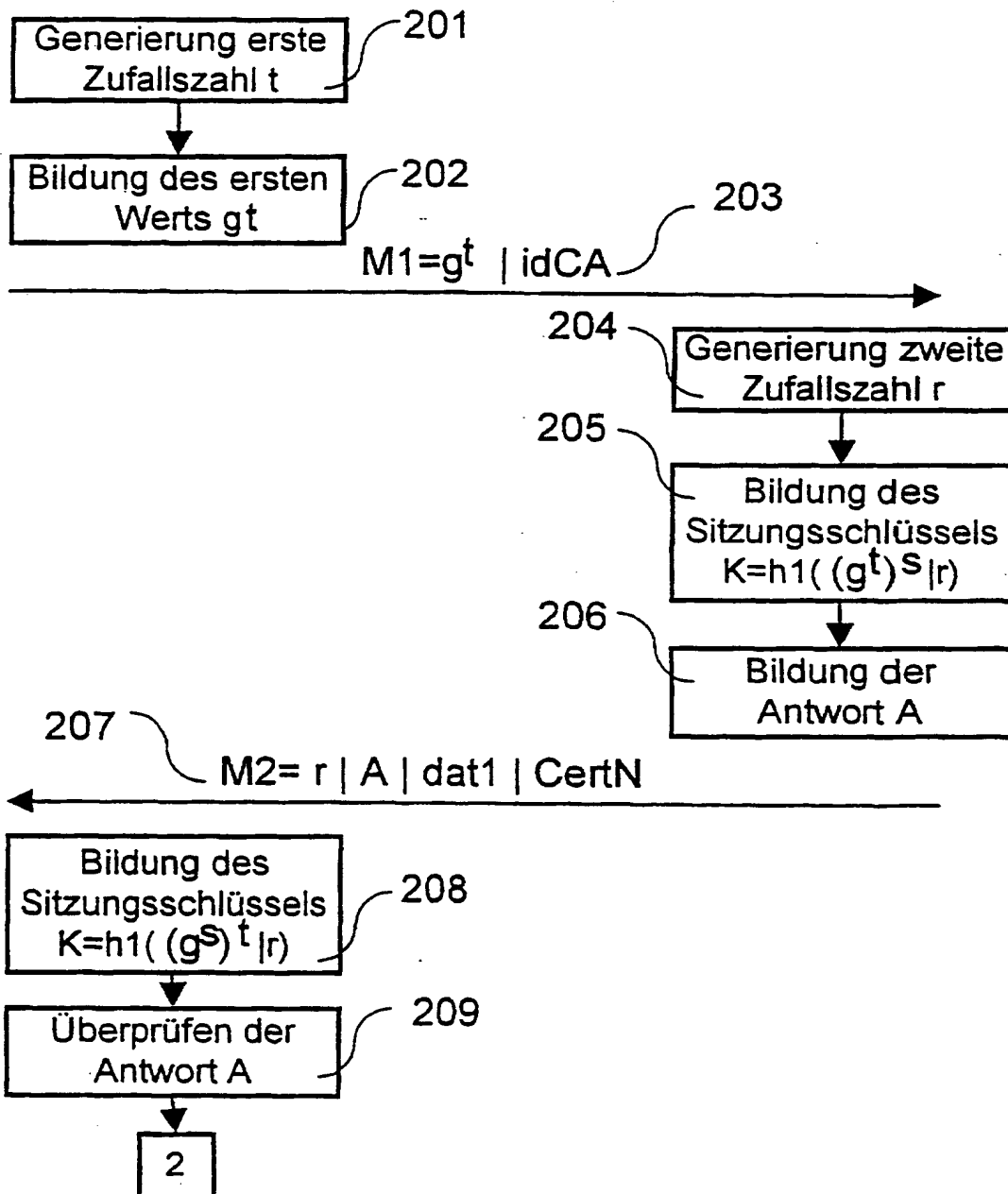
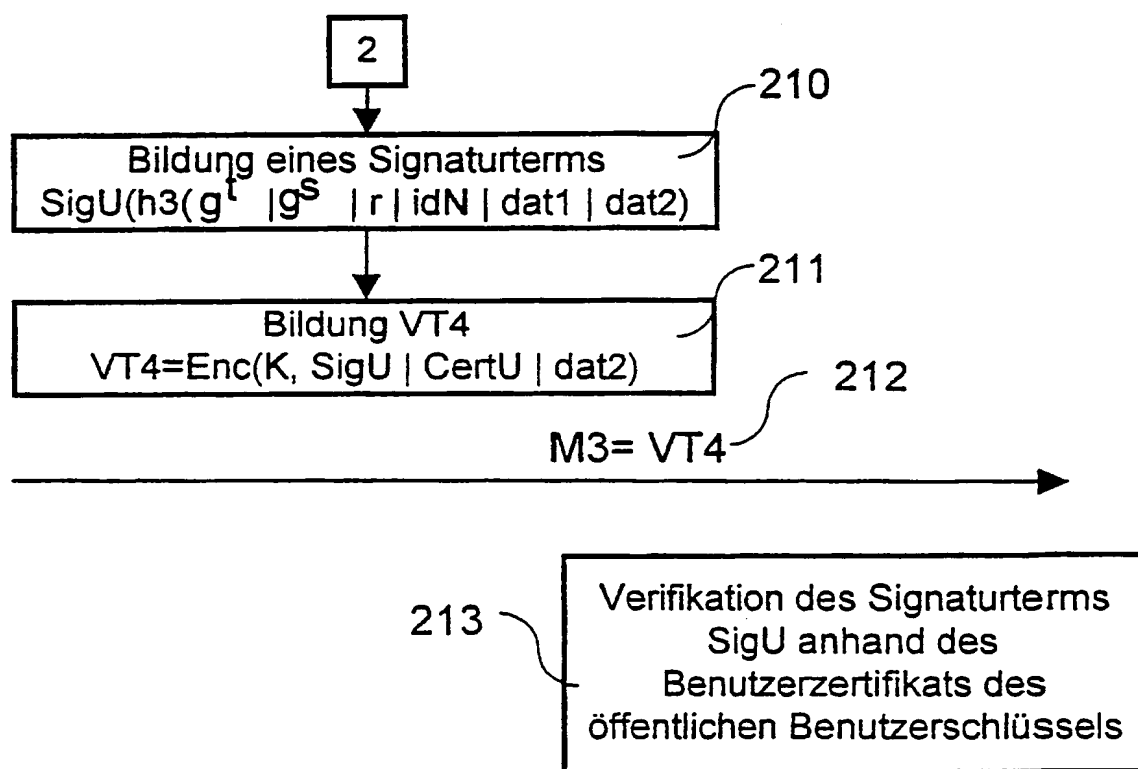
 g^S 

FIG 2B

erste Computereinheit U

zweite Computereinheit N



5/6

09/700928

FIG 3A

erste Computereinheit U Zertifizierungscomputereinheit CA
 g^U zweite Computereinheit N

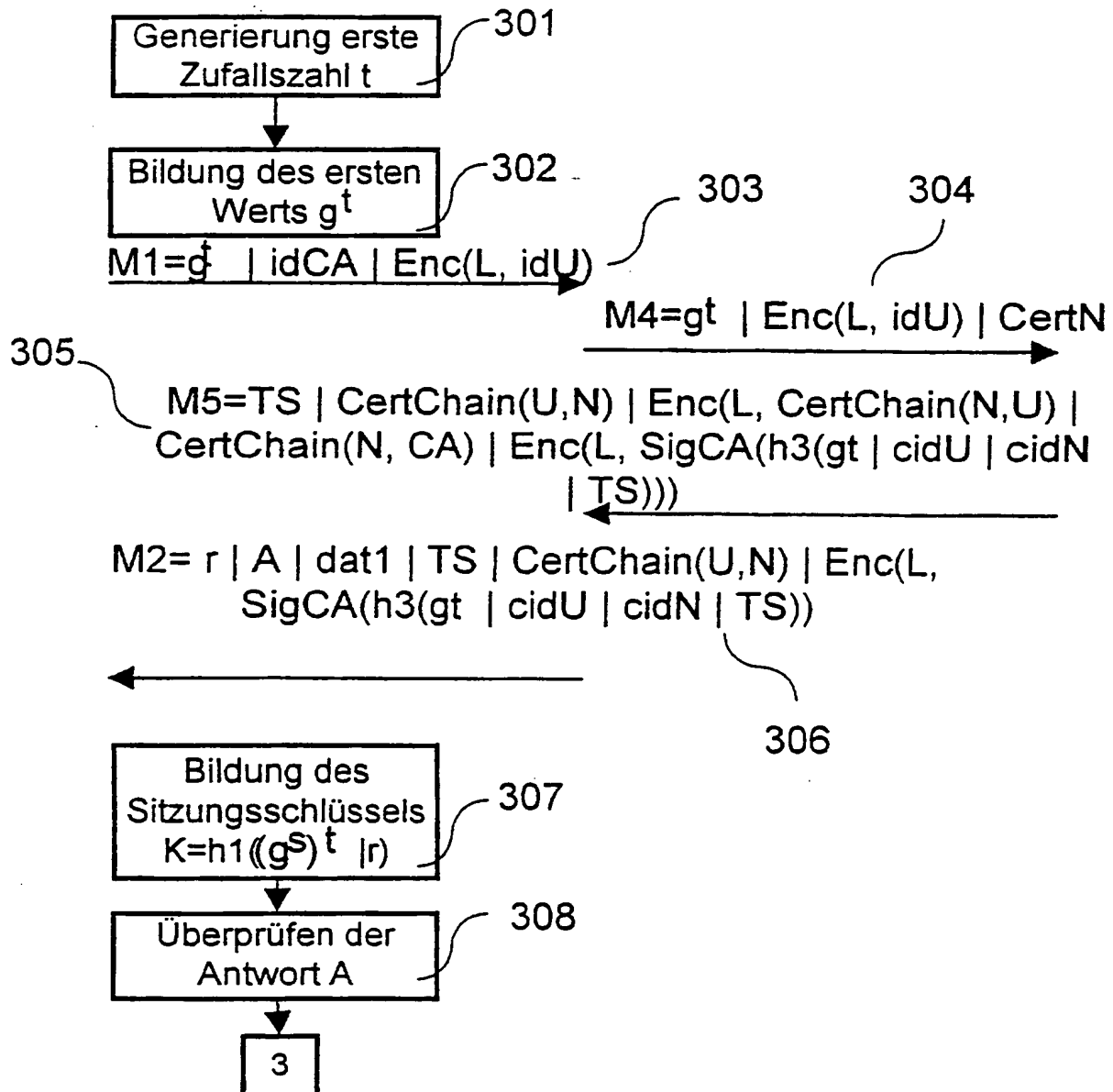
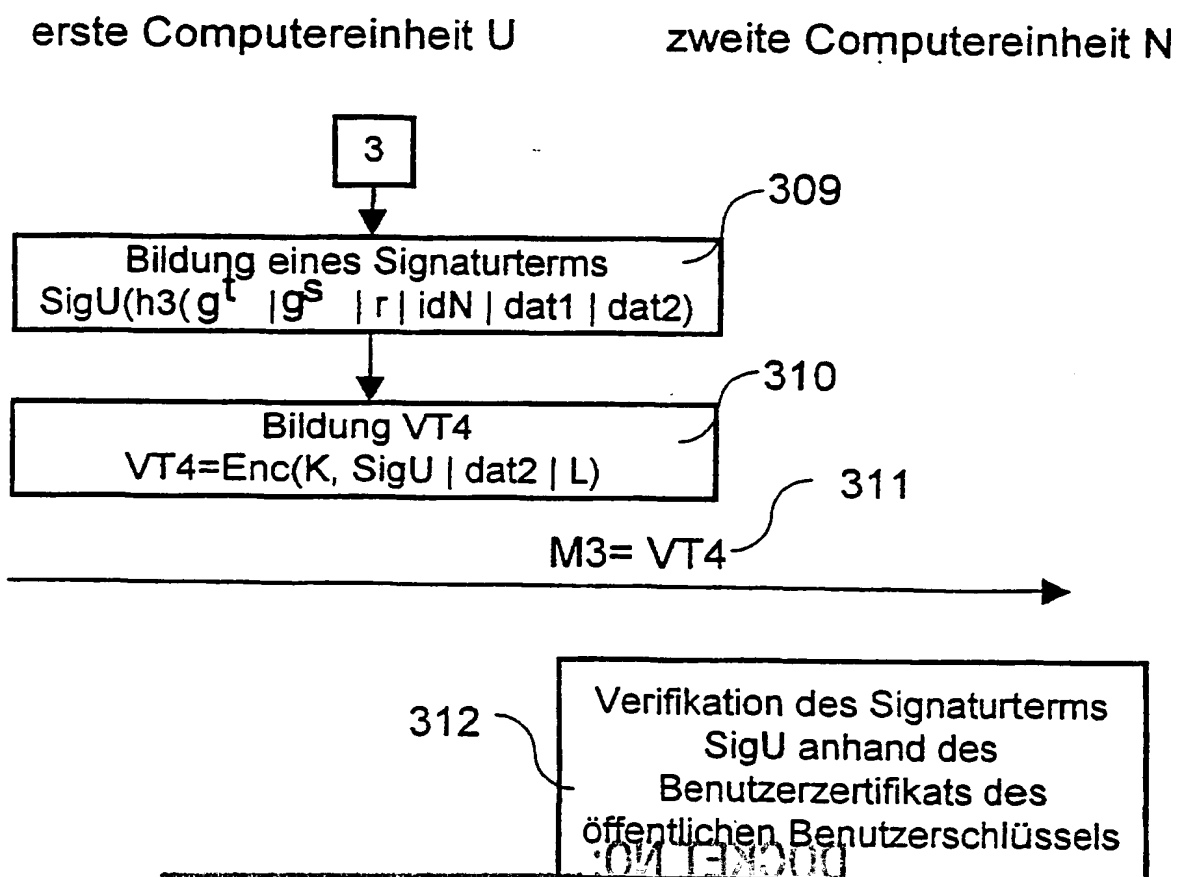


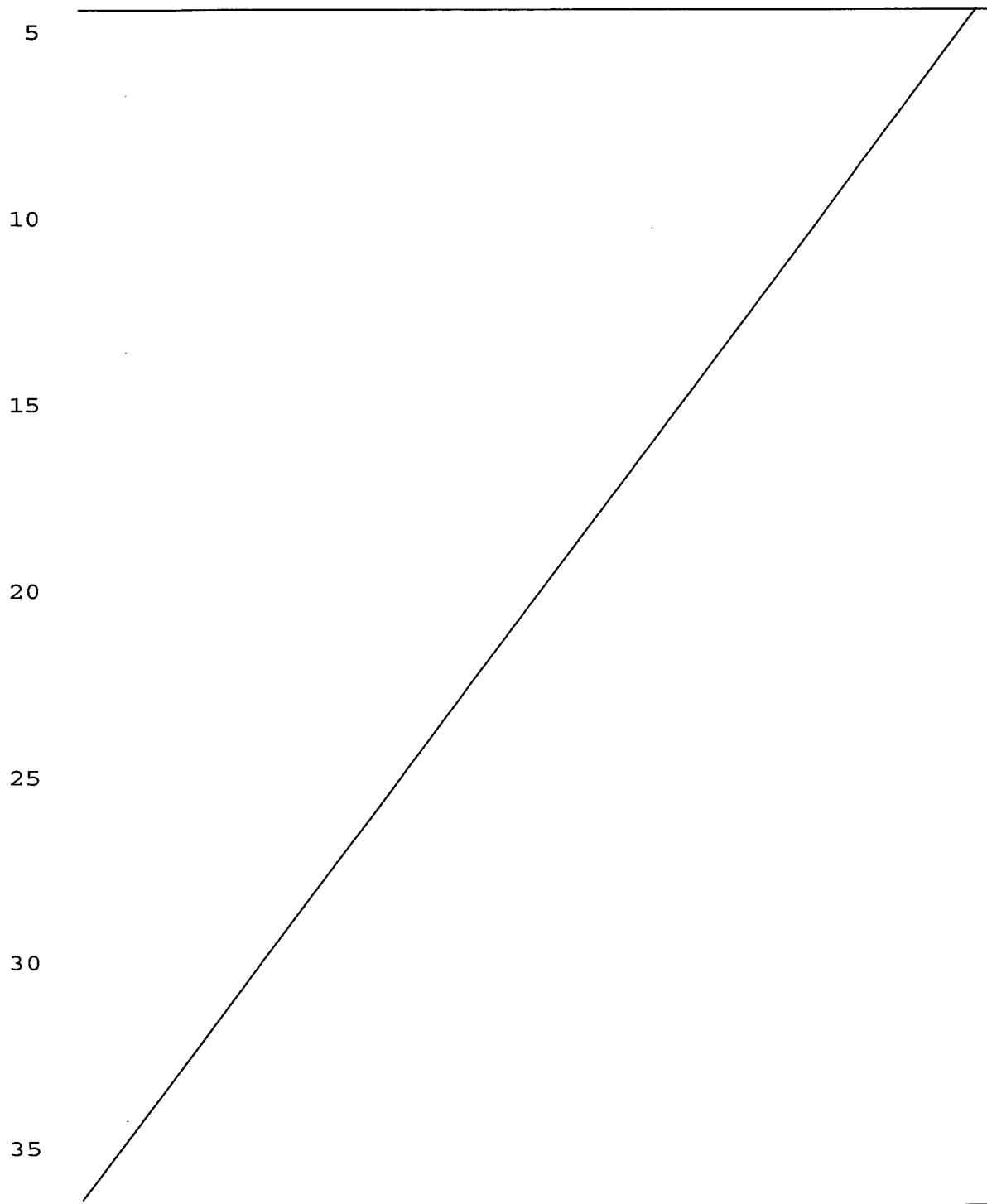
FIG 3B



Patent claims

1. A method for the computer-aided interchange of cryptographic keys between a first computer unit (U) and a second computer unit (N),
- 5 - in which a first value (g^t) is formed from a first random number (t) using a generating element (g) of a finite group in the first computer unit (U),
- 10 - in which a first message (M1) is transmitted from the first computer unit (U) to the second computer unit (N), the first message (M1) containing at least the first value (g^t),
- 15 - in which a session key (K) is formed in the second computer unit (N) using a first hash function (h1), a first input variable for the first hash function (h1) containing at least one first term which is formed by exponentiation of the first value (g^t) using a secret network key
- 20 (s),
- in which the session key (K) is formed in the first computer unit (U) using the first hash function (h1), a second input variable for the first hash function (h1) containing at least one
- 25 second term which is formed by exponentiation of a public network key (g^s) using the first random number (t),
- in which a fourth input variable is formed in the first computer unit (U) using a second hash function (h2) or the first hash function (h1), a
- 30 third input variable for the first hash function (h1) or for the second hash function (h2) containing, for the purpose of forming the fourth input variable, one or more variables
- 35 which can be used to infer the session key unambiguously, at least part of the variable being a nonpublic variable,

- in which a signature term is formed in the first computer unit (U) from at least the fourth input variable using a first signature function (Sig_U),



5

10

15

20

25

30

the first message (M1) containing at least the first value (g^t),

- a session key (K) is formed in the second computer unit (N) using a first hash function (h1), a first input variable for the first hash function (h1) containing at least one first term which is formed by exponentiation of the first value (g^t) using a secret network key (s),

35

- 5 - the session key (K) is formed in the first computer unit (U) using the first hash function (h1), a second input variable for the first hash function (h1) containing at least one second term which is formed by exponentiation of a public network key (g^s) using the first random number (t),
- 10 - a fourth input variable is formed in the first computer unit (U) using a second hash function (h2) or the first hash function (h1), a third input variable for the first hash function (h1) or for the second hash function (h2) containing, for the purpose of forming the fourth input variable, one or more variables which can be
- 15 used to infer the session key unambiguously, at least part of the variable being a nonpublic variable,
- 20 - a signature term is formed in the first computer unit (U) from at least the fourth input variable using a first signature function (Sig_U),
- 25 - a third message (M3) is transmitted from the first computer unit (U) to the second computer unit (N), the third message (M3) containing at least the signature term from the first computer unit (U), and
- the signature term is verified in the second computer unit (N).

30 33. The arrangement as claimed in claim 31,

35

in which the secret network key and/or the public network key is/are long-service keys.

34. The arrangement as claimed in claim 32 or 33,

FIG 1A

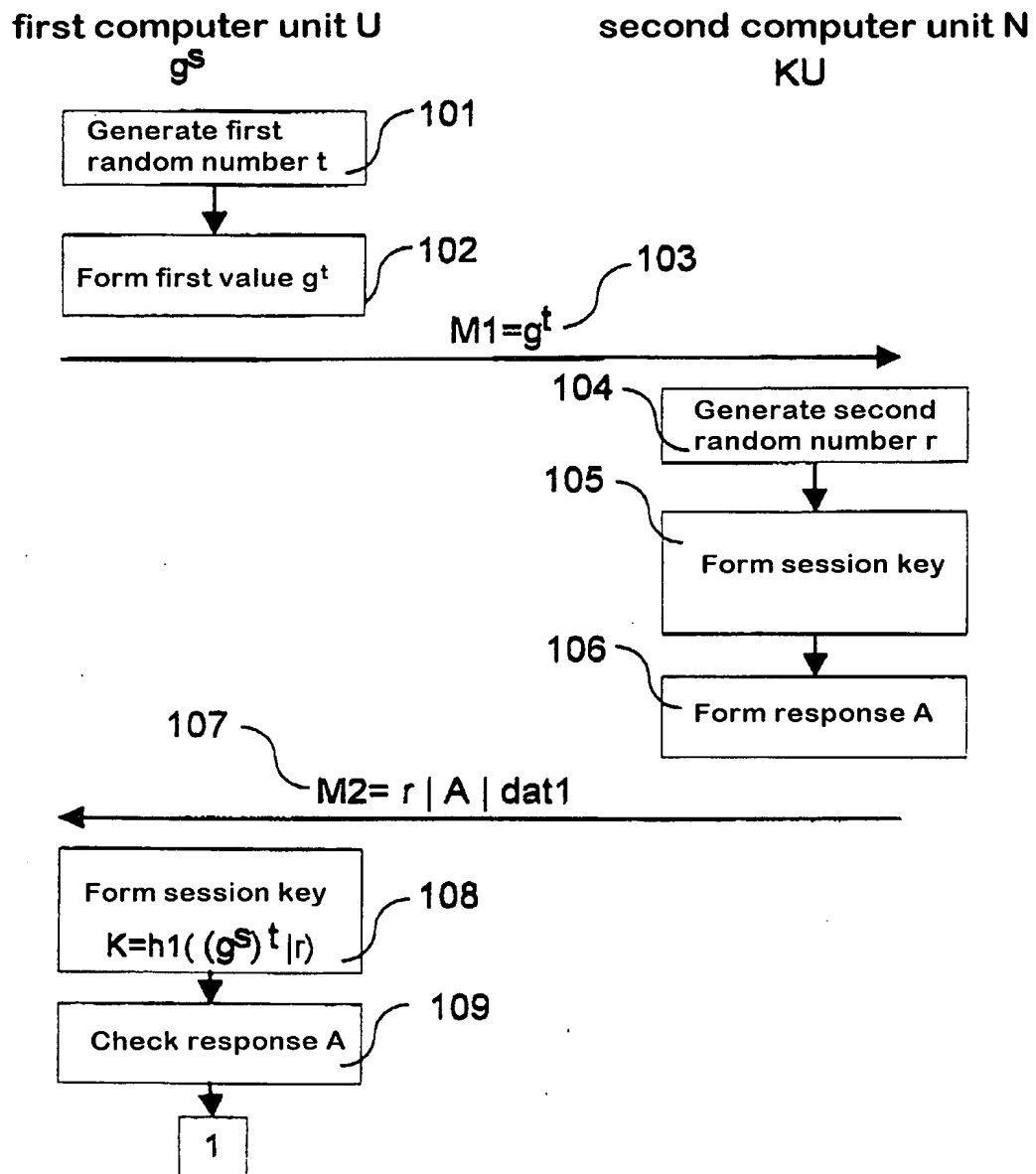


FIG 1B

first computer unit U

second computer unit N

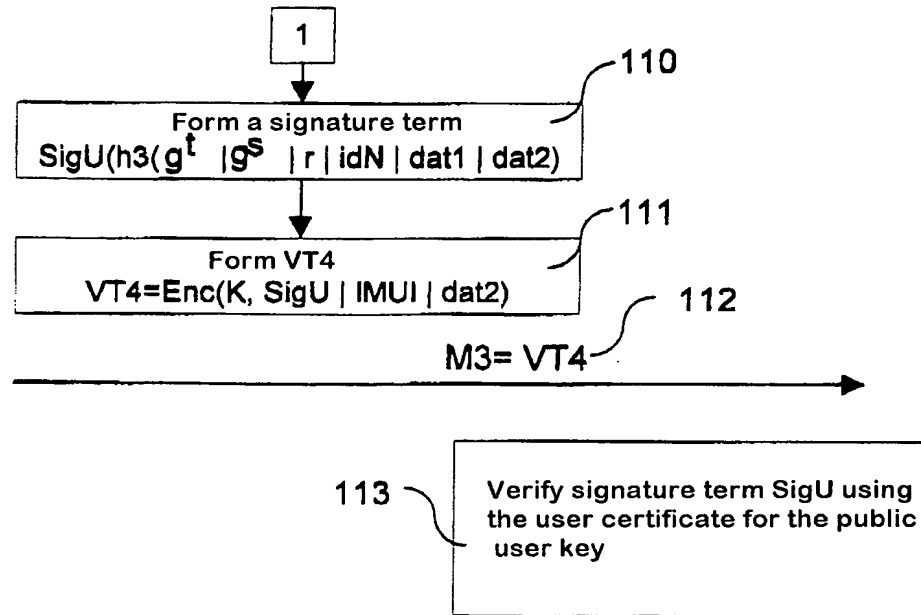


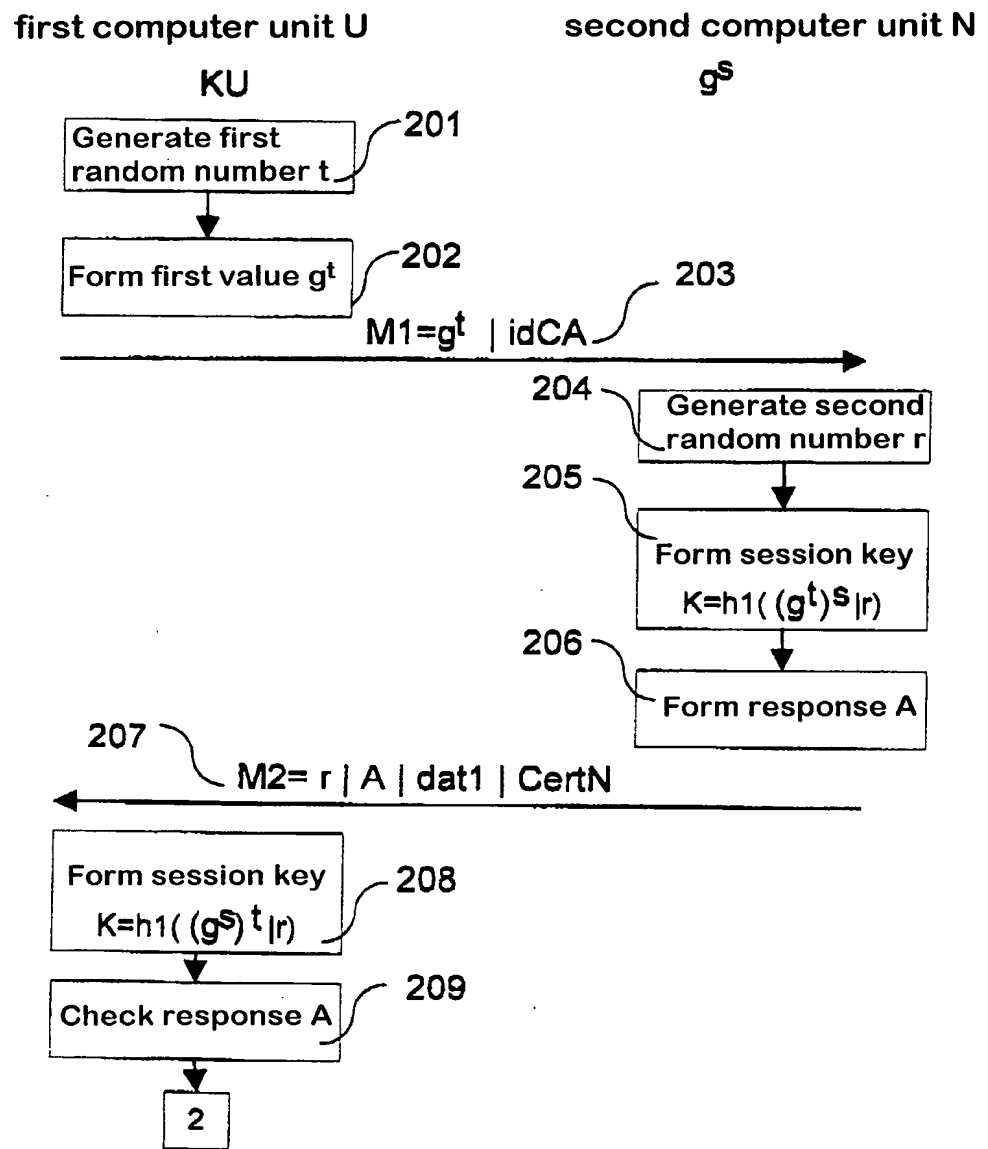
FIG 2 A

FIG 2B

first computer unit U

second computer unit N

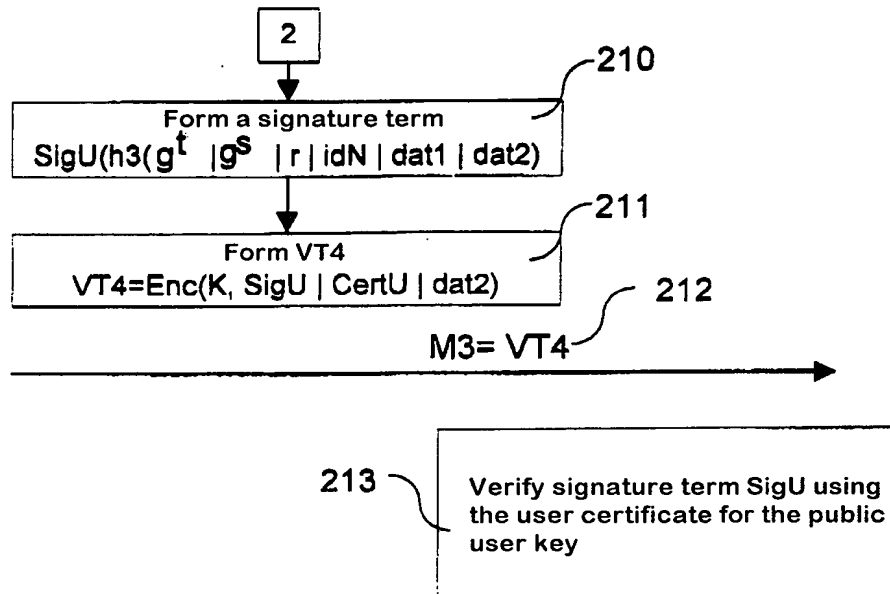


FIG 3 A

first computer unit U certification computer unit CA
 g^u second computer unit N

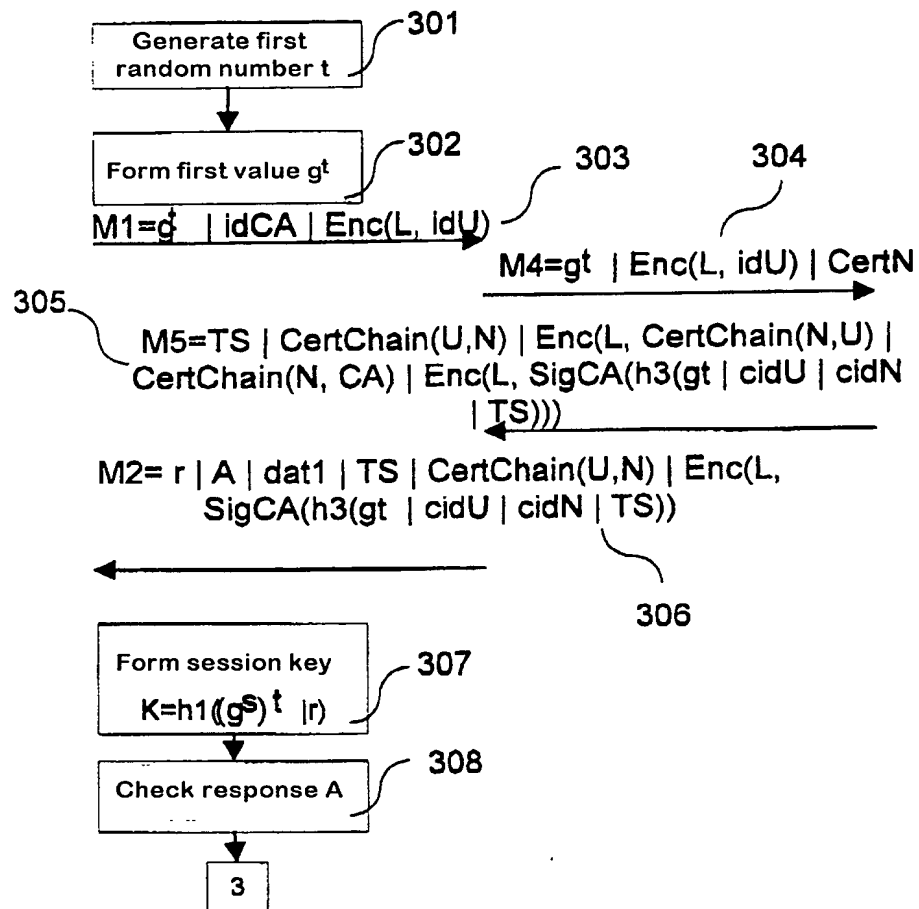


FIG 3B

first computer unit U

second computer unit N

